

BILLY J. WILLIAMS, OSB #901366
United States Attorney
District of Oregon
ETHAN D. KNIGHT, OSB #992984
GEOFFREY A. BARROW
CRAIG J. GABRIEL, OSB #012571
Assistant United States Attorneys
ethan.knight@usdoj.gov
geoffrey.barrow@usdoj.gov
craig.gabriel@usdoj.gov
1000 SW Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Attorneys for United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

UNITED STATES OF AMERICA

3:16-CR-00051-BR

v.

AMMON BUNDY, et al.,
Defendants.

**GOVERNMENT'S RESPONSE TO
DEFENDANTS' MOTION TO COMPEL
NOTICE OF SURVEILLANCE AND FOR
PRODUCTION OF RELATED
DISCOVERY (#545)**

The United States of America, by Billy J. Williams, United States Attorney for the District of Oregon, and through Ethan D. Knight, Geoffrey A. Barrow, and Craig J. Gabriel, Assistant United States Attorneys, hereby responds to defendants' Motion to Compel Notice of Surveillance and for Production of Related Discovery (ECF No. 545), filed by defendant O'Shaughnessy on behalf of all defendants.

I. Government's Position

Although this case is complex for many reasons, the discovery provided to date reflects evidence obtained using only regular criminal investigation authorities. There is nothing in this

case suggesting that any evidence in this investigation was collected by the U.S. Intelligence Community using non-criminal intelligence authorities pursuant to Executive Order (“E.O.”) 12333. Nor have defendants made the showing necessary to require the government to do anything further under 18 U.S.C. § 3504. Litigating this Motion, and attempting to imply that the broader U.S. intelligence community has any involvement in this case, is an unnecessary waste of court resources at a time while all parties are actively working to keep this case on track for its scheduled trial date. Defendants’ Motion should be denied without oral argument.

II. Legal Argument

By this Motion, defendants seek an order requiring the government “(1) to provide notice of its use of Executive Order 12333 – whether for gathering intelligence or to obtain evidence for use in this criminal prosecution, and (2) to delineate the fruits of any such surveillance.” (Defs.’ Mem. 1-2, ECF No. 545-1). They further request an order directing the U.S. Attorney’s Office to inquire of various agencies of the Intelligence Community concerning “any use of Executive Order 12333 in investigating these defendants.” (Defs.’ Mem. 2). Because there is absolutely nothing to indicate that this investigation or prosecution involved anything other than a normal, albeit high-profile, domestic criminal investigation, the defendants’ Motion should be denied without hearing.

A. This Prosecution Stems from Criminal Investigative Authorities

During the course of the occupation of the Malheur Refuge, as well as afterwards, criminal investigators led by the FBI sought and obtained evidence of defendants’ crimes. Law enforcement officers monitored television news and public social media platforms while the defendants publicly incriminated themselves. Law enforcement obtained criminal search

warrants for automobiles, online accounts, and digital devices seized at the Refuge or incident to arrest. They obtained court orders for pen register/trap and trace devices. They obtained court orders for information concerning stored electronic communications.

To date, the government has turned over approximately 43,700 pages and roughly 2 terabytes in discovery. This discovery includes, *inter alia*, search warrants, pen register/trap and trace orders, 18 U.S.C. § 2703(d) orders obtained by the government during the course of the investigation, and the evidence obtained as a result of those orders. It also includes evidence obtained while monitoring the defendants as they broadcasted their crimes on television news, on YouTube, and on other social media platforms. The discovery contains video obtained during aerial surveillance by law enforcement officers, the results obtained from cameras placed on telephone poles, and statements of witnesses interviewed by FBI agents.

Counsel for the government are aware of the government's obligation to produce discovery in accordance with Fed. R. Crim. P. 16 and applicable case law. The discovery in this case provides and will continue to provide evidence collected through a variety of criminal investigative techniques and court orders authorizing the collection of such evidence and data when required by law. If there had been any interception of wire, oral, or electronic communications, as defined in 18 U.S.C. § 2510 (commonly referred to as a Title III wiretap), in this investigation, the government would have already provided defense counsel with the relevant Title III applications and orders. There were no such orders issued in this investigation, and we are unaware of any Title III electronic surveillance of these defendants.

Additionally, whether or not defendants may be called "domestic terrorists," or whether they have been so criticized by politicians, Defs.' Mem. 5-7, their investigation and prosecution

for the unlawful Malheur Refuge occupation matter does not involve “*international* terrorism” as that term is defined under federal law. *See* 18 U.S.C. § 2331(1). As such, they could not properly be targeted as part of any effort to obtain foreign intelligence. *See* 50 U.S.C. § 1801 (defining terms such as “foreign power” and “foreign intelligence” for purposes of the Foreign Intelligence Surveillance Act (“FISA”)). FISA itself makes clear that any effort to target a U.S. person for electronic surveillance must be conducted pursuant to a FISA order (or, if for ordinary law enforcement purposes, pursuant to Title III). *See* 50 U.S.C. §§ 1801(f)(1), 1812 (providing that FISA and other provisions of the criminal code are the exclusive means through which electronic surveillance, defined to include surveillance targeting U.S. persons in the United States, may be conducted); 50 U.S.C. § 1881c(a)(2) (requiring a FISA order to conduct electronic surveillance targeting any U.S. person who is outside the United States); *see also* E.O. 12333, § 2.5 (any effort to target a U.S. person for electronic surveillance for intelligence purposes must be conducted in accordance with FISA). If the government had engaged in electronic surveillance or physical searches of the defendants pursuant to FISA and planned to use evidence obtained or derived from such electronic surveillance or physical searches in court against an aggrieved person as defined under FISA, the government would be under an obligation to notify such aggrieved person. *See* 50 U.S.C. §§ 1806(c) and 1825(d). No such notice has been given to the defendants in this matter, nor does the government plan on giving such notice to the defendants.

None of the evidence or any court order produced has anything to do with E.O. 12333. E.O. 12333 is the organizing document which assigns different responsibilities to various components of the U.S. Intelligence Community such as the National Security Agency (“NSA”) and the Central Intelligence Agency. Those agencies collect foreign intelligence and

counterintelligence overseas concerning foreign powers. Again, nothing about the defendants' conduct concerns foreign powers or foreign intelligence. The purpose of E.O. 12333 is to collect "necessary information on which to base decisions *concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats.*" E.O. 12333, § 1.1. (emphasis added). E.O. 12333 also specifically instructs the intelligence community "to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." *Id.* § 1.1(b). It does not purport to organize or to direct domestic criminal investigations by law enforcement, and it expressly notes that it "shall not be construed to authorize any activity in violation of the Constitution or statutes of the United States." *Id.* § 2.8.

B. Title 18 U.S.C. § 3504 Does Not Require Any Further Response

Nor does 18 U.S.C. § 3504 support defendants' claim for more specific responses concerning alleged electronic surveillance. That section, provides in relevant part:

In any trial, hearing, or other proceeding in or before any court . . .

(1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act [defined elsewhere as the unlawful use of an electronic surveillance device] or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act.

Even assuming that section 3504 applies to electronic surveillance directed at non-U.S. persons overseas, a defendant must make out a prima facie case of such surveillance to trigger an affirmative duty for the government to respond. But "[a] party's right to learn of illegal surveillance is not absolute. '[B]ecause responding to ill-founded claims of electronic surveillance would place an awesome burden on the government, a claim of government electronic surveillance

of a party must be sufficiently concrete and specific’ before the government must respond.”

United States v. Waters, 627 F.3d 345, 364 (9th Cir. 2010) (quoting *United States v. Tobias*, 836 F.2d 449, 452-53 (9th Cir. 1988)); *see also United States v. Wylie*, 625 F.2d 1371, 1375-76 (9th Cir. 1980); *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1973).

In *Alter*, the Ninth Circuit set forth requirements to establish a prima facie case, including the presentation of specific facts supporting the possibility of such electronic surveillance, the dates of such supposed surveillance, the specific telephone numbers allegedly subjected to such surveillance, and facts establishing some connection between the alleged surveillance and the issue at hand under litigation. 482 F.2d at 1025-26. The rationale for requiring this prima facie case was explained later by the court as follows:

In *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1973), we required that the government’s reply to a party’s claim under § 3504 be ‘factual, unambiguous and unequivocal.’ However, because responding to ill-founded claims of electronic surveillance would place an awesome burden on the government, a claim of government electronic surveillance of a party must be sufficiently concrete and specific before the government’s affirmance or denial must meet the requirements of *Alter*, *supra*. Accordingly, a general claim requires only a response appropriate to such a claim. *See United States v. Vielguth*, 502 F.2d 1257 (9th Cir. July 17, 1974).

United States v. See, 505 F.2d 845, 856 (9th Cir. 1974). Here, defendants fail to make out any prima facie case at all.

Defendants begin with a tautology: since there is nothing in the discovery to suggest involvement by the greater intelligence community in this investigation, such involvement must have occurred but the prosecutors have been kept in the dark by the FBI via “parallel construction.” (Defs.’ Mem. 3-4). If such a claim were sufficient, the intelligence community’s files would have to be searched in every criminal case.

Defendants further suggest their case is established by media articles about NSA's disclosed surveillance programs generally, Defs.' Mem. 8-11, though none of the articles relate specifically to the defendants or this case. They do not provide any evidence or reason to believe that NSA intercepted their communications specifically. Defendants do not identify what exculpatory or otherwise discoverable material NSA might hold. Defendants do not explain what information not already in their possession or readily available to them might be contained within any communications held by NSA. No one articulates with any specificity how any hypothetical communications would be helpful to the defense. In short, the defendants' request amounts to mere speculation. *Cf. Waters*, 627 F.3d at 365 (the government had no further obligation to respond to a § 3504 request where the request was "neither concrete nor specific" and the defendant's "motion relied only on generalized statements about government surveillance programs").

Finally, defendants selectively quote from the Attorney General's Guidelines for Domestic FBI Operations concerning the use of "all of the FBI legal authorities" being available "for deployment in all cases to which they apply to protect the public from crimes and threats to the national security." (Defs.' Mem. 11). Defendants ignore the significance of the use of the terms "legal" authorities and "all cases to which they apply." The Guidelines do not authorize the FBI to use foreign intelligence collection authorities in all domestic criminal investigations. Rather, they recognize that there may be overlap when the FBI is investigating a crime that also involves a threat to "national security," defined as:

international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or

persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order.

Attorney General Guidelines for Domestic FBI Operations, 2008, at 7 (emphasis added). Again, defendants bark up the wrong tree, even conceding as much: “[I]t is not clear whether the FBI considers itself able to engage in direct surveillance of defendants as potential ‘terrorists’ under E.O. 12333.” (Defs.’ Mem. 15).

In *United States v. McDavid*, No. CR S–06–35 MCE, 2007 WL 926664 (E.D. Cal. Mar. 27, 2007), a defendant was charged with conspiracy to damage or destroy property with fire and explosives. He claimed he was considered to be a member of ELF or ALF and deemed a “domestic terrorist.” Alleging that such a designation made him a possible target of the NSA or of the FBI’s misuse of its “terrorist powers,” he sought discovery of “electronic communications information and material, such as call data, e-mail and internet activity” and “any and all information, data and material obtained through warrantless surveillance conducted by government agencies, including the NSA.” *Id.* at *1. The court denied the motion:

[B]efore a court may order disclosure, the defense must make a prima facie showing of materiality: Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense. . . . Nevertheless, defendant has made no showing of materiality. As noted above, he has speculated that there may be impeachment material in any intercepted communications involving the co-defendants and the confidential informant, but this is merely a “general description” insufficient to satisfy his burden under the rule.

2007 WL 926664, at *3-4 (citations omitted).

Moreover, even assuming *arguendo* that an intelligence agency such as the NSA possessed information concerning the defendants, that information is not in the possession of the prosecution

team or anyone acting on its behalf. Under its *Brady* obligations, the prosecution has a duty to search for and turn over all exculpatory, material evidence to a defendant. Under Rule 16 the government must disclose a defendant's written or recorded statements that are "within the government's possession, custody or control." Fed. R. Crim. P. 16. But those obligations extend only to those agencies or individuals who have "act[ed] on the government's behalf in the case." *Kyles v. Whitley*, 514 U.S. 419, 437 (1995).

Under *Brady*, *Kyles*, and their progeny, the government is not required to search the files of agencies of the Intelligence Community because they were not and are not "acting on the government's behalf in [this] case."¹ There has been no joint investigation with NSA or any other intelligence agency in this case. No intelligence agency collaborated with the prosecution team at any point in the investigation, and the prosecution has no reason to suspect that NSA or any other intelligence agency has any information relevant to this case.

As the court found in *United States v. McDavid*, *supra*:

This court need not determine the nature of defendant's burden on pretrial discovery or whether his general allegations satisfy that burden, however, because he faces another hurdle. Evidence is in possession of the government if it is in possession of cooperating agencies . . . or if the prosecutor has knowledge of and access to the documents. . . . Although defendant discusses the NSA's activities at length, he has failed to link them to this prosecution or to make any sort of showing that the prosecutor has knowledge of and access to any results of the

¹ *United States v. Shryock*, 342 F.3d 948, 983 (9th Cir. 2003) (citing *United States v. Santiago*, 46 F.3d 885, 893-94 (9th Cir. 1995) ("Prosecutors must turn over *Brady* materials when the [federal] prosecutors have knowledge of and access to the documents sought by the defendant."); *United States v. Zuno-Arce*, 44 F.3d 1420, 1427 (9th Cir. 1995) ("[T]he prosecutor is 'deemed to have knowledge of and access to anything in the custody or control of any federal agency participating in the same investigation of the defendant.'") (quoting *United States v. Bryan*, 868 F.2d 1032, 1036 (9th Cir. 1989)). No case categorizes an agency of the intelligence community that has played no part in the investigation or prosecution of a defendant as acting on the government's behalf in the case or as a part of the prosecution team.

NSA's surveillance. Defendant claims that the Joint Terrorism Task Force participated in the underlying investigation, but offers nothing apart from speculation to connect that group to the NSA's warrantless electronic surveillance and data mining. Accordingly, on this record, defendant has not made a sufficient showing to justify an order based on *Brady*.

2007 WL 926664, at *2. For similar reasons, the court also denied defendant's motion based on Rule 16. *Id.* at *3. *See also United States v. Simpson*, No. 13-CR-6025CJS, 2016 WL 285176, at *14 (W.D.N.Y. Jan. 22, 2016) (denying motion for discovery of NSA interceptions in a drug conspiracy case since NSA not part of the prosecution team).

III. Conclusion

For the reasons given above, the defendants' Motion to Compel Notice of Surveillance and for Production of Related Discovery should be denied without a hearing.

Dated this 25th day of May 2016.

Respectfully submitted,

BILLY J. WILLIAMS
United States Attorney

s/ *Ethan D. Knight*
ETHAN D. KNIGHT, OSB #992984
GEOFFREY A. BARROW
CRAIG J. GABRIEL, OSB #012571
Assistant United States Attorneys